

UNITED STATES DISTRICT COURT

for the
Central District of California

In the Matter of the Search of)
)
the person of ASHOT AVANISIAN) Case No. 2:23-MJ-00313
("AVANISIAN")
)
)
)
)
)
)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

See Attachment A

located in the Central District of California, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
21 U.S.C. § § 841(a)(1) and 846
18 U.S.C. § § 1791 and 2

Offense Description
See attached Affidavit

The application is based on these facts:

See attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (*give exact ending date if more than 30 days: _____*) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Zachary A. Sumpter

Applicant's signature

Zachary A. Sumpter, TFO USPIS

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: _____

Judge's signature

City and state: Los Angeles, CA

Honorable Michael Wilner, U.S. Magistrate Judge

Printed name and title

AUSA: Lyndsi Allsop, ext. 3165

ATTACHMENT A

PERSON TO BE SEARCHED

The person of ASHOT AVANISIAN ("AVANISIAN"), date of birth 01/16/1995, with California Driver's License Number F3207846. AVANISIAN's California Department of Motor Vehicle records list him as standing 5' 7" tall with a bald head and brown eyes.

The search of AVANISIAN shall include any and all clothing and personal belongings, digital devices, backpacks, wallets, briefcases, purses, and bags that are within AVANISIAN's immediate vicinity and control at the location where the search warrant is executed.

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 21 U.S.C. § 841(a)(1) (possession with intent to distribute controlled substances), 21 U.S.C. § 846 (conspiracy and attempt to distribute controlled substances), 18 U.S.C. § 1791 (providing and possessing contraband in prison), 18 U.S.C. § 2 (aiding and abetting), and 18 U.S.C. § 371 (conspiracy) the "Subject Offenses"), namely:

a. Any controlled substance, controlled substance analogue, or listed chemical;

b. Items and paraphernalia for the manufacturing, distributing, packaging, sale, or weighing of controlled substances, including scales and other weighing devices, plastic baggies, food saver sealing devices, heat sealing devices, balloons, packaging materials, containers, and money counters;

c. Items used in the packaging of currency for consolidation and transportation, such as money-counting machines, money wrappers, carbon paper, rubber bands, duct tape or wrapping tape, plastic wrap or shrink wrap, and plastic sealing machines;

d. United States currency over \$1,000 or bearer instruments worth over \$1,000 (including cashier's checks, traveler's checks, certificates of deposit, stock certificates, and bonds) (including the first \$1,000), and data, records, documents, or information (including electronic mail, messages

over applications and social media, and photographs) pertaining to, obtaining, possessing, using, applications for, or transferring money over \$1,000, such as bank account records, cryptocurrency records and accounts;

e. Documents and records reflecting the identity of, contact information for, communications with, or times, dates or locations of meetings with co-conspirators, sources of supply of controlled substances, or drug customers, including calendars, address books, telephone or other contact lists, pay/owe records, distribution or customer lists, correspondence, receipts, records, and documents noting price, quantities, and/or times when drugs were bought, sold, or otherwise distributed, whether contained in hard copy correspondence, notes, emails, text messages, photographs, videos (including items stored on digital devices), or otherwise;

f. Records, documents, programs, applications and materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

g. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show SMS text, email communications or other text or written communications sent to or received from any of the digital devices and which relate to the above-named violations;

h. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications, or other text or written communications sent to or received from any digital device and which relate to the above-named violations;

i. Audio recordings, pictures, video recordings, or still captured images related to the purchase, sale, transportation, or distribution of drugs;

j. Contents of any calendar or date book;

k. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations; and

e. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

f. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software,

as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. applications, programs, software, documentation, manuals, passwords, keys, and other access devices that may be necessary to access the device or data stored on the device, to run software contained on the device, or to conduct a forensic examination of the device;

vii. records of or information about Internet Protocol addresses used by the device.

2. As used herein, the terms "records," "information," "documents," "programs," "applications," and "materials" include records, information, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony

PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the scope of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase," "Griffeye," and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

d. If the search determines that a digital device does not contain any data falling within the scope of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the scope of items to be

seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the scope of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the

custody and control of attorneys for the government and their support staff for their independent review.

6. During the execution of this search warrant, law enforcement is permitted to: (1) depress AVANISIAN's thumb and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of AVANISIAN's face with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

7. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AFFIDAVIT

I, Zachary A. Sumpter, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of an application for a warrant to search the person of ASHOT AVANISIAN ("AVANISIAN") as described more fully in Attachment A.

2. The requested search warrants seek authorization to seize evidence, fruits, or instrumentalities of violations of 21 U.S.C. § 841(a)(1) (possession with intent to distribute controlled substances), 21 U.S.C. § 846 (conspiracy and attempt to distribute controlled substances), 18 U.S.C. § 1791 (providing and possessing contraband in prison), 18 U.S.C. § 2 (aiding and abetting), and 18 U.S.C. § 371 (conspiracy) the "Subject Offenses"), as described more fully in Attachment B. Attachments A and B are incorporated herein by reference.

3. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested search warrant and does not purport to set forth all my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only. All dates and times are approximate.

II. BACKGROUND OF AFFIANT

4. I am a Task Force Officer ("TFO") with the United States Postal Inspection Service ("USPIS") and have been so employed since November 2021. I am currently assigned as a TFO to the Contraband Interdiction and Investigations South Team of the Los Angeles Division, which is responsible for investigating drug trafficking violations involving the United States Mail. As such, I am an "investigative or law enforcement officer" of the United States within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Title 18, United States Code, Section 2516.

5. Prior to being assigned as a TFO with USPIS, I worked patrol as a full-time sworn law enforcement officer with the Chino Police Department. I have been a sworn law enforcement officer since August 2013. I am a police officer within the meaning of Section 830.1 of the California Penal Code.

6. I have received training and have experience investigating violations of state and federal narcotics and money laundering laws, including, but not limited to Title 21, United States Code, Sections 841, 846, 952, 959 and 963 and Title 18, United States Code, Section 1956(a).

7. I have been involved in various electronic surveillance methods including state and federal wiretap investigations, the debriefing of informants and witnesses, as well as others who have knowledge of the manufacturing,

distribution, transportation, storage, and importation of controlled substances and the laundering of drug proceeds.

8. I am familiar with narcotics traffickers' methods of operation, including the manufacturing, storage, transportation, and distribution of narcotics, the collection of money that represents the proceeds of narcotics trafficking, and money laundering. I am also familiar with the ways that narcotics traffickers transport and distribute narcotics in areas they control. I am familiar with how drug traffickers use counter-surveillance techniques to avoid law enforcement detection. I also know that drug traffickers often communicate with their associates through cellular telephones. I have become aware that more sophisticated drug trafficking networks now utilize the dark web, e-mail, Voice Over Internet Protocol, video chat, internet messaging services, and social networking sites to communicate with one another. During drug-related communications, traffickers often use coded or cryptic language to disguise the drug-related nature of their conversations.

III. SUMMARY OF PROBABLE CAUSE

9. USPIS is investigating the introduction of approximately 3.1017 grams of heroin into Metropolitan Detention Center, Los Angeles ("MDC LA"), which was hidden in a parcel addressed to SEVAK MEHRABIAN ("MEHRABIAN") through the United States mail.

10. On or about July 1, 2022, while MEHRABIAN was imprisoned, he initiated a call to AVANISIAN and then instructed AVANASIAN to call an unidentified male who MEHRABIAN referred to

as "Pete." During the call, the three men discussed shipping heroin using coded language.

11. On July 7, 2022, the mail room staff at MDC LA discovered a suspicious envelope containing a book addressed to MEHRABIAN. Upon further inspection, the mail room staff located heroin in the spine of the book.

12. On July 18, 2022, MEHRABIAN was interviewed by a member of the Federal Bureau of Prison's Special Instigative Services ("SIS"), Abel Delgado. During the interview, MEHRABIAN admitted to attempting to introduce drugs into MDC LA.

13. On July 27, 2022, I took possession of the heroin and drug parcel wrappings. On July 29, 2022, the heroin, book, and drug parcel wrappings were sent to the USPIS Forensic Lab for chemistry and latent print analysis. The controlled substance in the book tested positive for heroin. No latent prints were recovered from the wrappings or the book.

14. I am seeking a warrant for AVANASIAN's person -- including digital devices thereon -- because I believe the below-stated facts constitute probable cause that evidence of the SUBJECT OFFENSES will be found there.

IV. STATEMENT OF PROBABLE CAUSE

15. Based on my review of law enforcement reports, conversations with other law enforcement agents, and my own knowledge of the investigation, I am aware of the following:

A. July 1, 2022: MEHRABIAN, AVANISIAN, and "Pete" Discuss Shipping Heroin Using Coded Language

16. Based on my review of a recorded phone call between MEHRABIAN, AVANISIAN, and "Pete," and a transcription and translation thereof, I know the following:

a. On or about July 1, 2022, MEHRABIAN, while imprisoned, initiated a call to AVANISIAN at 818-641-9530 (the "9530 Number").¹

b. During the phone call, MEHRABIAN instructed AVANISIAN to call his former "celly"² "Pete" at 760-899-0947 (the "0947 Number").³

c. AVANISIAN dialed the 0947 Number, and once the three men were all on the line, they had, in relevant part the following conversation:

PETE: Yeah, who is this.

MEHRABIAN: Pete.

PETE: What's happening, who is this?

MEHRABIAN: It's Slick. A, I was going to ask you, remember that letter⁴ you wrote for me when I was your celly [inaudible].

¹ T-Mobile subscriber information indicated that this number is registered to Karine Avanian.

² Based on my training and experience, the term "celly" is code for a former cellmate, meaning, an individual who someone was housed with while they were both imprisoned.

³ Sprint PCS subscriber information indicated that this number is registered to Gilbert Martinez.

⁴ Based on my training, experience, and review of the evidence in this case, I believe that the letter MEHRABIAN is referring to is a letter that was found in his cell by SIS, which gave detailed instructions on how to conceal drugs in a book, described further below in Section IV.E.

PETE: Yeah, yeah.

MEHRABIAN: This homie that just called you with this number, after I hang up can you explain that to him.

PETE: I sure can.

MEHRABIAN: Alright my boy, good looking. If anything, if he can't get the hang of it, could you meet up with him or I don't know.

PETE: Yeah, if he can come down to the Valley, I available right now or whenever.

. . .

MEHRABIAN: Alright, I'll see what he can do, just save that number and then he will call you later.

17. Based on my training and experience and my review of the phone call and its transcription and translation, I believe that the purpose of the phone call was for MEHRABIAN to ask "Pete" to explain to AVANISIAN on how to conceal drugs into a book and to ship it into a prison, and further, that during the call, "Pete" agreed to explain the process to AVANISIAN.

B. July 5, 2022: AZNARAN Mails a Parcel from a United States Post office to MEHRABIAN at MDC LA

18. Based on my review of surveillance footage from a United States Post Office located at 241 W Rialto Avenue, Rialto, California 92376 (the "Rialto Post Office"), I know the following:

a. On July 5, 2022, at approximately 3:05 p.m., AZNARAN entered the Rialto Post Office with a parcel in his left hand.

b. AZNARAN had a shaved head and was wearing a white t-shirt with camouflage shorts.

c. AZNARAN waited in line until the clerk assisted him.

d. AZNARAN placed the parcel on the countertop and paid the shipping fee with cash.

e. At approximately 3:08 p.m., AZNARAN exited the post office.

19. Based on my review of postal records, I know that the parcel AZNARAN dropped off at the Rialto Post Office was addressed to "SEVAK MEHRABIAN 41968-509, MDC Los Angeles, P.O. Box 531500, Los Angeles CA 90053." The return address was listed as "Say It Twice Books, 17400 Arrow Blvd, Fontana CA 92335."

C. Identification of AZNARAN

20. Using law enforcement databases, I identified AZNARAN by comparing his California driver's license photograph with the surveillance footage and determined that AZNARAN was the shipper.

D. July 7, 2022: MDC LA Mail Staff Discover the Heroin Concealed in a Package Mailed to MEHRABIAN

21. Based on my review of an MDC LA SIS report written by Abel Delgado and Joseph Rendo I know the following:

a. On July 7, 2022, at approximately 11:05 a.m., mail room staff at MDC LA discovered a suspicious envelope containing a book addressed to MEHRABIAN.

b. Upon further inspection, mail staff discovered a black tar like substance, measuring approximately four inches in length was in the spine of the book.

c. The then-unknown substance weighed 3.9 grams.

d. The substance was tested utilizing a NIK test kit A, U, and K, which gave a positive reading for Morphine.

E. July 2022: SIS Discovers a Letter with Instructions Regarding how to Conceal Heroin in a Book in MEHRABIAN's Cell

22. Based on my review of an MDC LA SIS report written by Abel Delgado and Joseph Rendo, and my own review of a copy of the letter found in MEHRABIAN's cell, I know the following:

a. MEHRABIAN had a letter in his cell that provided instruction on how to conceal contraband, specifically "black," which based on my training and experience, is code for heroin, in a book.

b. The letter contained pictures demonstrating how to conceal "black" in a book and it also contained the following instructions:

i. ". . .[P]ut five strips on each page and glue it with the second page, between two pages and stick them to the book. Put five new strips, put orderly on the side of the second page and let it stick properly. And remember, we should be able to open that page in a finger-length stance from the bottom side, so the people working here don't have any

suspicious, when the cop takes and quickly opens and shakes to see if something falls from there or not."

ii. "Put glue in here that line is drawn and then close the second page on it till it sticks good then shake the book to make sure the strips don't fall out. So, for example start on page 13. Put very little glue around the strips as close as you can to the inner edge of the book. Then put very little glue around the strips in a tiny line and make sure it normal glue stick you are using. Then pull page 14 over it till the glue tries. Then skip 10 pages and do it again till you have all of it done. If you putting black, make sure it is a hard cover book that you buy and carefully cut the side from inside and take the piece of hard cardboard out of the side and make the black the same size and shape and put back in its place and use the glue to glue it back. But this time use string glue. Then right away open the book and use blade to cut out the dry glue that's holding it together."

23. Based on my review of MEHRABIAN's July 1, 2022 phone call with "Pete" and AVANISIAN, specifically, the following excerpt, I believe that "Pete" wrote the letter found in MEHRABIANS's cell.

MEHRABIAN: A, I was going to ask you, remember that letter you wrote for me when I was your celly. . .

PETE: Yeah, yeah.

MEHRABIAN: This homie that just called you⁵ with this number, after I hang up, can you explain that to him.

F. July 18, 2022: Interview of MEHRABIAN

24. Based on my review of an MDC LA SIS report written by Abel Delgado and Joseph Rendo, I know the following:

a. On July 18, 2022, at approximately 6:45 a.m., SIS Delgado interviewed MEHRABIAN.⁶

b. During the interview, MEHRABIAN admitted that he attempted to bring drugs into the prison, however, he refused to disclose any outside person who mailed the "unknown substance."⁷

c. During the interview, MEHRABIAN stated that he will take full responsibility and does not want anyone else being held responsible.

G. August 1, 2022: Analysis of the Black Tar-Like Substance Found in the Book Shipped to MEHRABIAN

25. Based on my review of a drug analysis report generated by USPIS Forensic Chemist David C. Huang, I know that Mr. Huang tested the substance concealed in the book shipped to MEHRABIAN and confirmed that it was 3.1017 grams of heroin (net weight).

⁵ I believe that MEHRABIAN is referring to AVANISIAN since he is the person who called "Pete."

⁶ There is no mention of SIS Delgado Mirandizing MEHRABIAN prior to interviewing him. At the time of this filing, I have not spoken with SIS Delgado and, therefore, I cannot state, with absolute certainty, whether MEHRABIAN was Mirandized.

⁷ The USPIS drug lab report was not completed at the time of the interview.

H. August 9, 2022: Latent Print Analysis of the Book

26. Based on my review of a latent print analysis report generated by Forensic Latent Print Analyst Kiandra R. Brown-Holliday I know that Ms. Brown-Holliday examined the book and wrappings for the presence of latent prints; however, no latent prints were present or developed.

V. TRAINING AND EXPERIENCE ON DRUG OFFENSES

27. Based on my training and experience and familiarity with investigations into drug trafficking conducted by other law enforcement agents, I know the following:

a. Drug trafficking is a business that involves numerous co-conspirators, from lower-level dealers to higher-level suppliers, as well as associates to process, package, and deliver the drugs and launder the drug proceeds. Drug traffickers often travel by car, bus, train, or airplane, both domestically and to foreign countries, in connection with their illegal activities to meet with co-conspirators, conduct drug transactions, and transport drugs or drug proceeds.

b. Drug traffickers often maintain books, receipts, notes, ledgers, bank records, and other records relating to the manufacture, transportation, ordering, sale, and distribution of illegal drugs. The records are often maintained where drug traffickers have ready access to them, such as on their cell phones and other digital devices, and in their residences.

c. Communications between people buying and selling drugs take place by telephone calls and messages, such as e-mail, text messages, and social media messaging applications,

sent to and from cell phones and other digital devices. This includes sending photos or videos of the drugs between the seller and the buyer, the negotiation of price, and discussion of whether participants will bring weapons to a deal. In addition, it is common for people engaged in drug trafficking to have photos and videos on their cell phones of drugs they or others working with them possess, as they frequently send these photos to each other and others to boast about the drugs or facilitate drug sales.

d. Drug traffickers often keep the names, addresses, and telephone numbers of their drug trafficking associates on their digital devices and in their residence. Drug traffickers often keep records of meetings with associates, customers, and suppliers on their digital devices and in their residence, including in the form of calendar entries and location data.

e. Drug traffickers often use vehicles to transport their narcotics and may keep stashes of narcotics in their vehicles in the event of an unexpected opportunity to sell narcotics arises.

f. Drug traffickers often maintain on hand large amounts of United States currency to maintain and finance their ongoing drug trafficking businesses, which operate on a cash basis. Such currency is often stored in their residences and vehicles.

g. Drug traffickers often keep drugs in places where they have ready access and control, such as at their residence or in safes. They also often keep other items related to their

drug trafficking activities at their residence, such as digital scales, packaging materials, and proceeds of drug trafficking. These items are often small enough to be easily hidden and thus may be kept at a drug trafficker's residence even if the drug trafficker lives with others who may be unaware of his criminal activity.

h. It is common for drug traffickers to own multiple phones of varying sophistication and cost as a method to diversify communications between various customers and suppliers. These phones range from sophisticated smart phones using digital communications applications such as Blackberry Messenger, WhatsApp, and the like, to cheap, simple, and often prepaid flip phones, known colloquially as "drop phones," for actual voice communications.

i. Based on my training and discussions with experienced Postal Inspectors, I know that Postal Inspectors have been conducting investigations of drug trafficking via USPS Express Mail and Priority Mail since the mid-1980s. In particular, they began conducting organized interdictions of Express Mail and Priority Mail parcels suspected of containing controlled substances and proceeds from the sale of controlled substances in Los Angeles, California, in the early 1990s. Along with conducting organized interdictions, Postal Inspectors also regularly examine and investigate Express Mail and Priority Mail parcels throughout the year. During the 1990s, Postal Inspectors observed that the trend was for drug traffickers to send controlled substances and proceeds from the sale of

controlled substances using boxes, with the proceeds in the form of cash. Although Postal Inspectors still see the use of boxes for controlled substances and cash, there has been a gradual change over the years toward the current trend of smaller boxes, flat cardboard envelopes, and Tyvek envelopes, with proceeds from the sale of controlled substances converted to money orders. Drug traffickers use the USPS delivery services because of their speed, reliability, and the ability to track the package's progress to the intended delivery point.

VI. TRAINING AND EXPERIENCE ON DIGITAL DEVICES⁸

28. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the

⁸ As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures

are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

29. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

30. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress AVANISIAN's thumb and/or fingers on the device(s); and (2) hold the device(s) in front of AVANISIAN's face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

31. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

VII. CONCLUSION

32. For all of the reasons described above, there is probable cause to believe that the items to be seized described in Attachment B will be found in a search of the person described in Attachment A.

Attested to by the applicant in
accordance with the requirements
of Fed. R. Crim. P. 4.1 by
telephone on this ____ day of
_____, 2023.

HONORABLE MICHAEL WILNER
UNITED STATES MAGISTRATE JUDGE